JOURNAL OF NUMBER THEORY 41, 146–149 (1992)

Normal Generators of Finite Fields

SAFWAN AKBIK

Department of Mathematics, Hofstra University, Hempstead, New York 11550

Communicated by Hans Zassenhaus

Received November 5, 1990; revised June 11, 1991

INTRODUCTION

Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements and δ be the automorphism which sends $\xi \in \mathbb{F}_{p^n}$ into ξ^p. A normal basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is one of the form

$$\alpha, \delta\alpha, \ldots, \delta^{n-1}\alpha, \tag{1}$$

for some $\alpha \in \mathbb{F}_{p^n}$. Such an α is called a normal generator of $\mathbb{F}_{p^n}$. It is known that every finite field has a normal basis. In 1968 Davenport [1] proved that $\mathbb{F}_{p^n}$ has a primitive normal basis, i.e., a basis (1) which satisfies the further condition that α generates the multiplicative group of $\mathbb{F}_{p^n}$. In the course of his proof Davenport obtained a lower bound for the number of normal generators.

In this paper we will derive an exact formula for the number $N(p^r)$ of (not necessarily primitive) normal generators.

THEOREM. *For each positive integer d with $(d, p) = 1$, define $O_d(p)$ to be the smallest positive integer such that*

$$p^{O_d(p)} \equiv 1 \pmod{d}.$$

Let n_0 be the integer defined by $n = p^s n_0$ with $(p, n_0) = 1$. Then the number $N(p^n)$ of normal generators of $\mathbb{F}_{p^n}$ is given by

$$N(p^n) = p^{n-n_0} \prod_{d \mid n_0} (p^{O_d(p)} - 1)^{\varphi(d)/O_d(p)}, \tag{2}$$

where φ is the Euler function.

Using formula (2) we will later prove the following corollary which gives Davenport's lower bound for $N(p^n)$.

0022-314X/92 $5.00

COROLLARY. *Let*

$$l = \sum_{d \mid n_0} \frac{\varphi(d)}{O_d(p)},$$

then the number of normal generators of $\mathbb{F}_{p^n}$ *is at least* $p^{n-1}(p-1)^l$ *and hence is at least* $(p-1)^n$.

To prove our theorem we will consider two lemmas.

For each $\alpha \in \mathbb{F}_{p^n}$, let $f_\alpha(\delta)$ be the least degree monic polynomial in $R[\delta, \mathbb{F}_p]$, the ring of polynomials in δ with coefficients in $\mathbb{F}_p$, such that

$$f_\alpha(\delta)\,\alpha = 0.$$

LEMMA 1. *Let* $g(\delta) \in R[\delta, \mathbb{F}_p]$ *with* $g(\delta) \mid \delta^n - 1$, *then the number of elements* $\alpha \in \mathbb{F}_{p^n}$ *such that*

$$f_\alpha(\delta) \mid g(\delta), \tag{3}$$

is $p^{\deg g(\delta)}$, *i.e.*,

$$\sum_{\substack{\alpha \in \mathbb{F}_{p^n} \\ f_\alpha(\delta) \mid g(\delta)}} 1 = p^{\deg g(\delta)}. \tag{4}$$

Proof. It is clear that $f_\alpha(\delta)$ divides $g(\delta)$ if and only if

$$g(\delta)\,\alpha = 0. \tag{5}$$

Thus the number of α satisfying (3) is the number of roots in $\mathbb{F}_{p^n}$ of Eq. (5). Since $g(\delta) \mid \delta^n - 1$, it follows that $g(\delta)\,x \mid (\delta^n - 1)\,x$. But $(\delta^n - 1)\,x = x^{p^n} - x$ which splits in $\mathbb{F}_{p^n}$; thus the number of roots of Eq. (5) is the degree of the polynomial $g(\delta)\,x$. But if $g(\delta) = \sum_{i=1}^{k} a_i \delta^i$, where $k = \deg g(\delta)$, then $g(\delta)\,x = \sum_{i=1}^{k} a_i x^{p^i}$. Thus the degree of $g(\delta)\,x$ is p^k. This proves the lemma.

LEMMA 2. *For a non-constant* $d(\delta)$ *in* $R[\delta, \mathbb{F}_p]$, *let* $\nu(d(\delta))$ *be the number of distinct monic irreducible factors of* $d(\delta)$. *Define* $\mu(1) = 1$, *and* $\mu(d(\delta))$ *as*

$$\mu(d(\delta)) = \begin{cases} (-1)^{\nu(d(\delta))} & \text{if } d(\delta) \text{ is square-free} \\ 0 & \text{if } d(\delta) \text{ is not square-free.} \end{cases} \tag{6}$$

Let $g(\delta)$ *denote a monic polynomial in* $R[\delta, \mathbb{F}_p]$. *Then*

$$\sum_{d(\delta) \mid g(\delta)} \mu(d(\delta)) = \begin{cases} 1 & \text{if } g(\delta) = 1 \\ 0 & \text{otherwise,} \end{cases} \tag{7}$$

where $d(\delta)$ *runs over* 1 *and all* (*non-constant*) *monic divisors of* $g(\delta)$.

Proof. If $g(\delta)$ is not 1 and if it has m ($m \geqslant 1$) distinct monic irreducible factors in $R[\delta, \mathbb{F}_p]$, then

$$\sum_{d(\delta) \mid g(\delta)} \mu(d(\delta)) = 1 - m + \binom{m}{2} - \binom{m}{3} + \cdots + (-1)^m$$
$$= (1-1)^m = 0.$$

Proof of the Theorem. Since for each $\alpha \in \mathbb{F}_{p^n}$, $(\delta^n - 1)\,\alpha = \alpha^{p^n} - \alpha = 0$, it follows that $f_\alpha(\delta) \mid \delta^n - 1$. In fact α is a normal generator if and only if $f_\alpha(\delta) = \delta^n - 1$. Then (7) implies that

$$N(p^n) = \sum_{\alpha \in \mathbb{F}_{p^n}} \sum_{d(\delta) \mid (\delta^n - 1)/f_\alpha(\delta)} \mu(d(\delta)). \tag{8}$$

Interchanging the order of summation in (8) we get

$$N(p^n) = \sum_{d(\delta) \mid \delta^n - 1} \mu(d(\delta)) \sum_{\substack{\alpha \in \mathbb{F}_{p^n} \\ f_\alpha(\delta) \mid (\delta^n - 1)/d(\delta)}} 1. \tag{9}$$

But by (4) we have

$$\sum_{\substack{\alpha \in \mathbb{F}_{p^n} \\ f_\alpha(\delta) \mid (\delta^n - 1)/d(\delta)}} 1 = p^{\deg((\delta^n - 1)/d(\delta))}$$
$$= p^{n - \deg d(\delta)}.$$

This and (9) give

$$N(p^n) = p^n \sum_{d(\delta) \mid \delta^n - 1} \mu(d(\delta))\, p^{-\deg d(\delta)}. \tag{10}$$

Since $\mu(d(\delta)) = 0$ when $d(\delta)$ is not a square-free, it follows that if $k_1(\delta)$, $k_2(\delta)$, ..., $k_r(\delta)$ are the distinct irreducible factors of $\delta^n - 1$ over $\mathbb{F}_p$, then (10) becomes

$$N(p^n) = p^n \sum_{d(\delta) \mid k_1(\delta) k_2(\delta) \cdots k_r(\delta)} \mu(d(\delta))\, p^{-\deg d(\delta)}. \tag{11}$$

By definition (6), it is easy to see that (11) can be written as

$$N(p^n) = p^n \prod_{i=1}^{r} (1 - p^{-\deg k_i}). \tag{12}$$

But since $n = p^s n_0$,

$$\delta^n - 1 = (\delta^{n_0} - 1)^{p^s} \pmod{p}$$
$$= \left(\prod_{d \mid n_0} \Psi_d(\delta) \right)^{p^s},$$

where $\Psi_d(\delta)$ is the cyclotomic polynomial of order d. W. J. Guerrier [3] showed that $\Psi_d(\delta)$ factors mod p into $\varphi(d)/O_d(p)$ distinct polynomials each of degree $O_d(p)$. Thus for each $d \mid n_0$, $\Psi_d(\delta)$ contributes

$$(1 - p^{-O_d(p)})^{\varphi(d)/O_d(p)}$$

to the product in (12). Thus (12) becomes

$$N(p^n) = p^n \prod_{d \mid n_0} (1 - p^{-O_d(p)})^{\varphi(d)/O_d(p)} \tag{13}$$
$$= p^n \prod_{d \mid n_0} [p^{-O_d(p)}(p^{O_d(p)} - 1)]^{\varphi(d)/O_d(p)}$$
$$= p^n \prod_{d \mid n_0} p^{-\varphi(d)} (p^{O_d(p)} - 1)^{\varphi(d)/O_d(p)}$$
$$= p^n p^{-\sum_{d \mid n_0} \varphi(d)} \prod_{d \mid n_0} (p^{O_d(p)} - 1)^{\varphi(d)/O_d(p)}. \tag{14}$$

But $\sum_{d \mid n_0} \varphi(d) = n_0$, so (14) takes the required form (2) and the proof of the theorem is completed.

Proof of the Corollary. Since $P_d(p) \geqslant 1$, (13) implies that

$$N(p^n) \geqslant p^n \prod_{d \mid n_0} (1 - p^{-1})^{\varphi(d)/O_d(p)} = p^n (1 - p^{-1})^l = p^{n-l}(p-1)^l;$$

hence the corollary.

References

1. H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–39.
2. L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* **73** (1952), 373–382.
3. W. J. Guerrier, The factorization of the cyclotomic polynomials mod p, *Amer. Math. Monthly* **75** (1968), 46.